

ABSTRACT

In a quantum key distributing method of the present invention, a communication apparatus on a reception side performs error correction using parity check matrixes for an LDPC code that have an extremely high error correction ability. In the quantum key distributing method of the present invention, a cyclic code syndrome generated by a communication apparatus on a transmission side and an estimated cyclic code syndrome generated based on an estimated word after error correction are compared to perform error detection for the estimated word.